REMARKS

The Final Office Action mailed July 18, 2008, considered claims 1–7, 9, 10, 21-27, 29 and 30. Claims 1–2, 4–7, 10, 21-22, 24-28 and 30 were rejected under 35 U.S.C. 102(b) as being anticipated by Network Working Groups, request for Comments 1948, "Defending Against Sequence Number Attacks", by Bellovin (May 1996) (hereinafter Bellovin). Claims 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin, in view of McKay, U.S. Patent Pub. No. 2002/0187788 (filed Jun. 7, 2002) (hereinafter McKay). Claims 9 and 29 were rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin, in view of Afek et al., U.S. Patent Pub. No. 2002/0083175 (filed Aug. 14, 2001) (hereinafter Afek). Claim 23 was rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin, in view of McKay, and further in view of Dickman et al., U.S. Patent No. 3,728,535 (filed Aug. 19, 1971) (hereinafter Dickman).[1]

By this response, claim 1 is amended such that claims 1–7, 9–10, 21–27, and 29–30 remain pending.[2] Claims 1 and 21 are independent claims which remain at issue. Support for the amendments may be found within Specification ¶¶ 34–41.[3]

As reflected in the claims, the present invention is directed generally toward generating initial sequence numbers in communication protocols to prevent the communications from being attacked while maintaining reliable data transfers. Claim 1 recites, for instance, in combination with all the elements of the claim, a method for generating initial sequence numbers. The method includes generating an intermediate value from a hash function initialized by a random key generated from a local secret and a connection identifier key including connection information. The intermediate value is calculated from the initialized hash function. A connection rate is detected for the local server. The connection rate is determined by detecting each connection to the server and a connection rate evaluator determining the number of connections per unit time. A variable amount is determined based upon the connection rate. The

[1] Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] The amendments and remarks presented herein are consistent with the information presented by telephone by patent attorney John Bacoch (reg. no. 59,890) and attorney Thomas Bonacci.

[3] However, it should be noted that the present invention and claims as recited take support from the entire Specification. As such, no particular part of the Specification should be considered separately from the entirety of the Specification.

variable amount is determined by at least comparing the connection rate to a threshold value and by choosing a random number between a minimum ISN increase per connection and a maximum ISN increase per connection. A monotonically increasing counter takes timer input and connection rate input and produces a fixed value and the variable amount which are combined to produce a random value. The random value and the intermediate value are then combined by a monotonically increasing mathematical function to produce an initial sequence number.

Claim 21 recites a computer program product embodiment of the method of claim 1

Each of the independent claims 1 and 21 were rejected under 35 U.S.C. § 102 as being anticipated by Bellovin.[4] The Applicants have now amended the claims and submit that the present invention as recited in the claims is distinct from that taught by Bellovin.

Bellovin, RFC 1948, is well-known to those of skill in the art and was known to the Applicants. There are indeed certain similarities between the goal of Bellovin and the present invention (i.e., secure ISN generation) and there are some similarities between the teachings of Bellovin and the present invention. Bellovin does not, however, anticipate each and every element of the present invention as recited in the claims and Bellovin fails to teach all the elements of claims 1 and 21 as being arranged as required by the claims.

Despite certain similarities, Bellovin teaches a method distinct from that taught and claimed by the present invention. Bellovin calculates an initial sequence number (ISN) from the formula:

$$\text{ISN} = \text{M} + \text{F(localhost, localport, remotehost, remoteport)}^{5}$$

In this formula, M is a "4 microsecond timer"[6] and the function F is a "cryptographic hash function of the connection-id and some secret data."[7] The present invention, on the other hand, calculates an ISN by combining an intermediate value and a random value using a monotonically increasing function. Further, the random value is created by combining a fixed value (based on time) and a variable amount based upon a connection rate. Bellovin combines only a timer with a hash function of a connection-id and some secret data. Because of the distinctions, the

[4] Office Communication p. 3 (paper no. 20080716, July 18, 2008).

[5] Bellovin p. 3.

[6] Bellovin p. 3.

[7] Bellovin p. 4 l. 3–5.

Applicants respectfully traverse the rejections (and have amended the claims to further point out the distinctions).[8]

In particular, the Office asserts that Bellovin p. 2 l. 25–33 teaches a monotonically increasing counter taking both timer and connection rate information as input. The Applicants respectfully disagree. Firstly, the cited portion of Bellovin is part of the discussion of the *problem* of ISN attacks. Both Bellovin and the present invention teach (different) methods for avoiding the problem discussed in the cited portion. Further, "Berkeley-derived kernels increment [the initial sequence number] by a constant every second, and by another *constant* for each new connection"[9] fails to teach connection *rate* information being used as input to the counter. The counter discussed in the cited portion increments a constant amount for each unit time and increments a constant amount for each connection. Incrementing a constant amount for each connection does not take the *rate* of connections as input – only the number of connections without regard to time.[10] The cited constant increment per connection would be the same whether 5 connections happened in one second or whether 5 connections happened in one hour. The present invention, in contrast, teaches and claims that the *rate* of connections is input to the counter (which, of course, would be different for 5 connections/second versus 5 connections/hour).

The Office asserts that Bellovin p. 2 l. 28–30 teaches detecting a connection rate for the local server.[11] The Office further asserts that "[the] counter is incremented on a per connection basis, accordingly, the connection rate is known."[12] The Applicants respectfully disagree. As discussed above, incrementing a counter on a per connection basis results only in a count of the connections, not the *rate* of connections. Note that 10 connections over a short time would necessarily result in different rate than the same 10 connections over a longer time – the present invention and claims make that distinction. Bellovin teaches only an increment based upon the connection count, not the connection rate. Since Bellovin teaches that the ISN is incremented by

[8] These distinctions are important, *inter alia*, as a rejection under 35 U.S.C. § 102 would require all the elements being arranged as required by the claim.

[9] Bellovin p. 2 l. 28–30 (emphasis added).

[10] A direct analogy is a car's odometer versus its speedometer. The odometer records a constant amount for each mile driven. The odometer, however, does not record the rate (i.e., speed) of each of the miles driven. The Bellovin passage increments a counter for each connection - much like a car's odometer - but it fails to determine the rate (i.e., speed) of connections.

[11] Office Comm. p. 4.

[12] Office Comm. p. 4.

a *constant* for each connection, any rate information is necessarily lost (i.e., the same constant would be used whether the next connection occurred at a rate of 1 connection per second or a rate of 1 connection per hour).

The Office asserts that Bellovin p. 3–4 and "ISN computed using

M + F(localhost, localport, remotehost, remoteport)"

teaches combing the intermediate value and the random value using a monotonically increasing mathematical function to generate the initial sequence number.[13] Bellovin calculates an initial sequence number (ISN) from the formula:

ISN = M + F(localhost, localport, remotehost, remoteport)[14]

In this formula, M is a "4 microsecond timer"[15] and the function F is a "cryptographic hash function of the connection-id and some secret data."[16] The Office further asserts that ISN = M + F(localhost, localport, remotehost, remoteport) "is a strictly increasing function."[17] Such an assertion is not supported by Bellovin. There is no requirement in Bellovin that the hash function be monotonically increasing. If the hash function were to decrease at some point greater than the timer were increasing, then the sum would, indeed, not be increasing. "[T]here is no connection, syntactic or semantic, between the sequence numbers used for two different connections."[18] There is no support within Bellovin which requires that ISN = M + F(localhost, localport, remotehost, remoteport) to be a monotonically increasing function. It is certainly possible that M + F(...) (i.e., timer + hash function) be other than a monotonically increasing sum.

The above distinctions notwithstanding, the Applicants have amended independent claim 1 (and whose limitations are incorporated into independent claim 21) to more particularly point out the present invention and the distinctions over Bellovin. The amendments now presented provide distinctions over Bellovin in addition to those discussed above. As Bellovin fails to teach each and every limitation of claims 1 and 21 and because Bellovin fails to teach all the elements of the claims as being arranged as required by the claims, a rejection under 35 U.S.C. § 102 in view of Bellovin would be improper and should be withdrawn. Accordingly, the

[13] Office Comm. p. 5.
[14] Bellovin p. 3.
[15] Bellovin p. 3.
[16] Bellovin p. 4 l. 3–5.
[17] Office Comm. p. 5.
[18] Bellovin p. 3.

Applicants respectfully request favorable reconsideration of independent claims 1 and 21 as they are now recited. The Applicants further respectfully request favorable reconsideration of each of the dependent claims in view of the above discussion and the amendments to the independent claims.

In view of the foregoing, Applicants respectfully submit that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicants acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicants reserve the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicants specifically request that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 17th day of October, 2008.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant
Customer No. 47973

RDN/JCJ/TMB:crb
2130591_1